REMARKS

This Amendment is responsive to the Final Office Action dated June 13, 2007. Applicant has added new claims 57-60. Claims 1-4, 6, 7, 9-17, 27, 29, 30, 35-39, 41, 42, 44-46, 53, 55 and 57-60 are pending upon entry of this Amendment.

Interview Summary

As a preliminary matter, Applicant thanks the Examiner for the telephonic phone interview dated August 6, 2007. Examiner Gillis, Mr. Sieffert and Ms. Grunwald participated in the interview. In the interview, the participants discussed Applicant's independent claim 1 in relation to the cited prior art, specifically U.S. Patent Application No. 2002/0083175 to Afek et al. No agreement was reached, but the Examiner agreed to further consider Applicant's arguments if submitted in writing.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1, 3, 4, 6, 7, 9-11, 14, 27, 30, 35, 37-39, 41-44, 53 and 55 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,473,863 to Genty et al. ("Gentry") in view of U.S. Patent Application No. 2002/0083175 to Afek et al. ("Afek") in view of U.S. Patent No. 6,092,113 to Maeshima et al. ("Maeshima"). In addition, the Examiner rejected claims 2 and 36 under 35 U.S.C. § 103(a) as being unpatentable over Genty in view of Afek in view of Maeshima, and further in view U.S. Patent Application No. 2003/0016679 to Adams et al. ("Adams"). The Examiner also rejected claims 12, 13, 45 and 46 under 35 U.S.C. § 103(a) as being unpatentable over Genty in view of Afek in view of Maeshima, and further in view of U.S. Patent Application No. 2002/0099854 to Jorgensen. Furthermore, the Examiner rejected claims 16, 17 and 29 under 35 U.S.C. § 103(a) as being unpatentable over Genty in view of Afek in view of Maeshima, and further in view of U.S. Patent No. 6,880,090 to Shawcross.

Applicant respectfully traverses the rejections. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Genty, Afek and Maeshima

Claim 1 requires establishing a packet tunnel between a first local area network and a second local area network, the packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network. In relevant part, claim 1 further requires, in response to a detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. Claim 1 also requires establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network. Claims 27, 35 and 53 contain similar limitations.

With respect to the features of independent claims 1, 27, 35 and 53, the Examiner stated that Genty teaches a tunnel between a source and destination, an attack detected, a secondary tunnel established with different addresses, and, upon detecting a network attack, canceling the bandwidth in the packet tunnel. The Examiner stated that Genty fails to teach several features of claim 1, including establishing new virtual private network service upon detecting the network attack by selecting an intermediate network device having a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. Instead, the Examiner relied on Afek for teaching these feature.

With respect to Afek, the Examiner stated that Afek teaches different networks, such as LANs, connected together, and data diverted to guard devices upon detection of an attack by routing data sent to a target device from the source device to the guard devices and then from the guard devices to the target device. The Examiner asserted that Genty and Afek are analogous because they are both related to network protection and that it would have been obvious to a person of ordinary skill in the art to use the guard devices and redirection taught in Afek with the system in Genty because enhanced protection from distributed denial of service attacks is provided. In addition, the Examiner stated that Maeshima teaches reserving bandwidth for every tunnel on the network. The Examiner asserted that Genty, Afek, and Maeshima are analogous art because they are related to virtual private network setup and that it would have been obvious to a

person of ordinary skill in the art to use the bandwidth reservation in Maeshima with the system in Gentry in view of Afek because it is possible to construct a VPN which enables assurance of bandwidth.

Genty, Afek and Maeshima, either singularly or in combination, fail to teach or suggest, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device in response to the detected network attack, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as required by Applicant's independent claims 1, 27, 35 and 53.

The Examiner appears to have misinterpreted the Afek reference in regards to Applicant's independent claims. First, Afek does not teach *selecting* a guard device in response to the detected network attack all. Second, directly counter to Applicant's claims, Afek does not disclose selecting a guard device having a network address from a network address space *other than the address space of the first local area network and the address space of the second local area network.* In this manner, Afek in combination with the other references fail to provide a solution that achieves many of the technical advantages of Applicant's claimed technique.

Afek describes a "protected area" within a distributed network that includes routers, guard machines, and servers (victims).[1] Upon detecting an attack from outside of the protected area network on a server within the "protected area," the Afek system diverts to guard devices any inbound traffic destined to that server:

> A guard machine is placed in each entry next to the border routers at this point. Upon receiving the alert of a possible attack on a victim all the border routers are set to forward all the traffic arriving from outside of the network (protected area) and whose destination IP address is the victim public IP address, to the guard machine which is placed next to them.[2]

[1] Afek, paragraph [0240].
[2] Afek, paragraph [0257].

Afek also describes diverting traffic destined to the public IP address of a server upon detecting an attack from within the protected area network.

> [W]hen the victim suspects that an attack is being applied, it declares itself to be at a large distance from the server (victim) public IP address. At the same time the guards would start to declare that they are at distance zero (or close to zero) from the server (victim) public IP address. This routing updates quickly spread in the protected area network, using the standard routing protocol.... Thus within seconds from these declarations all the traffic whose destination is the victim public IP address, is automatically diverted to the guards.[3]

First, Afek makes no suggestion of *selecting* a guard machine in response to the detected network attack. Instead, Afek discloses that for attacks from outside of the protected area, routing information is updated to so that traffic is naturally from the border routers to the guard machines that are placed next to it at the entry to the protected area.

Second, Afek does not describe selecting a guard machine having a network address from a network address space *other than the address space of the first local area network and the address space of the second local area network.* Instead, Afek discloses that upon detecting a network attack, the guard machines declare that they have the **same public IP address as the victim** and within zero or a very small number of next hops from the public IP address. In turn, the victim declares that it is a very large number of next hops from the public IP address. In this way, the guard machine closest to the public IP address of the victim operates as a proxy for the victim server. **Thus, the Afek solution requires that the guard devices are located within the same protected area as the victim so that the guard devices are capable of taking the public IP address of the victim.** Only in this way can the guard devices operate as proxies for victim so as to divert traffic from the victim to the guard devices.

As an example, Figure 4b of Afek illustrates a triple handshake between a router, a guard machine, and a server (victim).

[3] Afek, paragraph [0258].

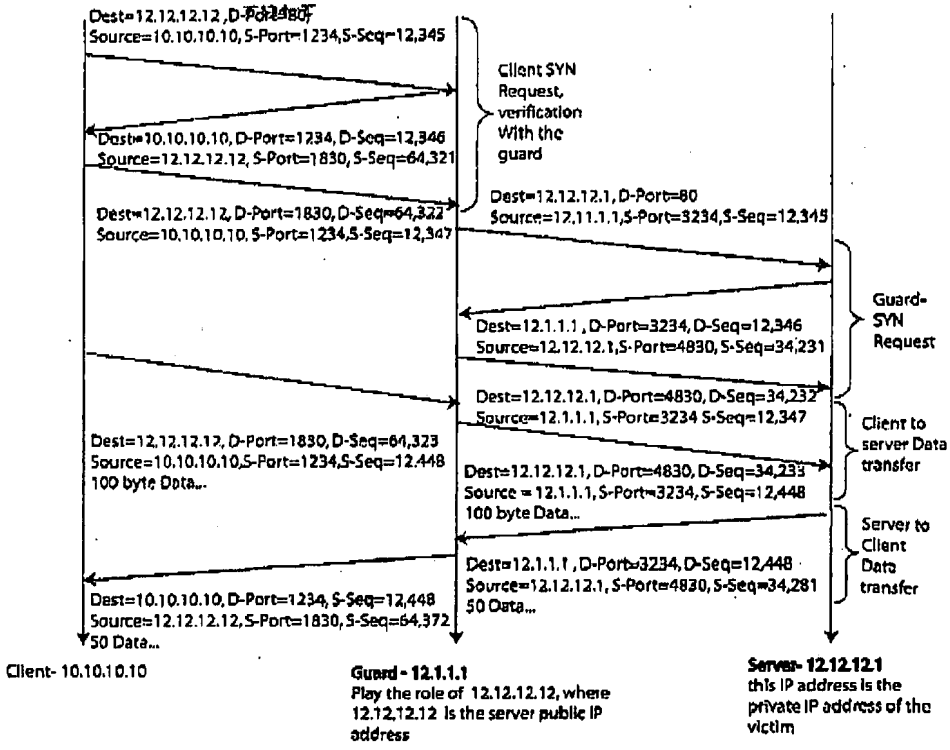

Figure 4b

As illustrated in Figure 4b of Afek, the guard machine **announces its public IP address to be the same and the public IP address of the victim server.** In this way, the guard machine "plays the role" of the server by accepting traffic from the router destined for the pubic IP address of the server. The guard machine then filters the received traffic and passes the trustworthy packets on to the victim server using the private IP address of the victim server. The guard device continues to act as a proxy for, or play the role of, the server by receiving packets from the server destined for the router.

According to the Afek reference, in order to divert traffic to a guard machine during an attack, the guard machine declares that is has the *exact same* public IP address as the server and then receives the traffic destined for the public IP address. Therefore, the guard machine does not operate as an intermediate device used to redirect traffic flowing between a first local area network to a second local area network in order to avoid the DDoS attack from the first local area network directed at the public IP address of a server within the second local area network. Instead, the guard machine of Afek is located within the protected area network and appears to

external devices as the victim server itself by declaring its public IP address to be the same as the public IP address of the victim server. In this way, the guard machine acts as a proxy for the victim server and continues to receive the DDoS attack directed at the public IP address of the victim server. The guard machine then filters all of the traffic destined for the public IP address of the victim server and forwards only the trustworthy packets to the victim server using its private IP address.

In response to Applicant's arguments filed April 30, 2007, the Examiner stated that Afek teaches the devices may be separated from each other in separate networks therefore having addresses in different address spaces. This analysis overlooks the requirements of the Afek solution. As illustrated in Figure 4b of Afek, the guard machine has a private IP address of 12.1.1.1 while playing the role of 12.12.12.12, which is the public IP address for the server, and the server has a private address of 12.12.12.1 and a public address of 12.12.12.12. Afek clearly teaches that the guard machine has a network address in the same address space as the server. Only in this way can the guard device declare that it has the same address of the victim. This solution is completely contrary to Applicant's independent claims 1, 27, 35 and 53, which recite the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network.

To further illustrate this point, if the guard machine in Afek declared that it had the same public IP address as the victim server but was somehow physically located in a different network area than the victim server, the guard device would then not be able to receive any traffic destined for the public IP address of the server. That is, traffic would not leave the protected area so as to be forwarded to the guard device. When a guard machine declares itself as having the same public IP address as the victim server, routing information for the protected area network is updated to reflect the declared next hop distance from the public IP address. Routers within the protected area network will then attempt to forward traffic destined for the public IP address of the victim server to the guard machine. However, if the guard machine is located in a different network area than the victim server, the traffic will not be able to reach the guard machine because the routers do not know how to route traffic destined for a local public IP address of the protected network if the guard device is in fact located in a different network area.

For at least these reasons, Afek in view of the other references does not teach or suggest a solution of establishing new virtual private network service upon detecting the network attack by selecting an intermediate network device having a network address from a network address space other than the address space of the first local area network and the address space of the second local area network as recited by Applicant's independent claims 1, 27, 35 and 53. As described above, Afek teaches that a guard machine may operate as a proxy for a victim server during a network attack by declaring the same public IP address as the victim server. Afek certainly does not disclose that the guard machine has a network address for a network address space other than the address space of the victim server, and does not provide any suggestion of any benefits achieved by such a system.

Thus, even if the teachings of Genty were modified by the teachings of Afek and Maeshima as suggested by the Examiner, the combined references would not result in Applicant's invention as claimed. For example, Genty in view of Maeshima would suggest establishing a secondary tunnel and entirely abandoning the original tunnel upon detecting a network attack, and reserving bandwidth for the new tunnel. Afek describes, upon detecting a network attack of a victim server, diverting traffic destined for the victim server from a router to a guard device that declares the same public IP address as the victim server. Combining the references would result at most in a system that, upon detecting a network attack, abandons the tunnel between the router and the victim server, establishes a new tunnel in its place between the router and the victim server, and diverts traffic from the router to the guard machine declaring the same public IP address as the victim server. The combined teachings fails to result in a system that splits a network tunnel between a first and second local area network by utilizing an intermediate device selected to have a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, as required by Applicant's independent claims 1, 27, 35, and 53.

For at least these reasons, Applicant's independent claims 1, 27, 35 and 53 are in condition for allowance, as are Applicant's dependent claims 3, 4, 6, 7, 9-17, 29, 30, 36-39, 41, 42, 44-46 and 55.

Genty, Afek, Maeshima and Adams

Applicant's dependent claims 2 and 36 recite that the source network address and the destination network address comprise port numbers. The Examiner acknowledged that Genty, Afek and Maeshima do not disclose the addresses comprising port numbers. However, the Examiner asserted that Adams teaches control information being an IP address or a port number amount other information. The Examiner stated that it would have been obvious to one of ordinary skill in the art to use control information described in Adams with the system of Genty, Afek and Maeshima because the packet is able to be sent to the next destination once the information is known.

As described above, Genty, Afek and Maeshima fail to disclose an intermediate network device that has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. Genty, Afek and Maeshima also fail to teach the remaining features of Applicant's independent claims 1 and 35. Adams provides no teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima. Neither Genty, Afek, Maeshima nor Adams disclose the features of Applicant's independent claims 1 and 35, which are in condition for allowance. For at least these reasons, Applicant's claims 2 and 36 which depend from claims 1 and 35, respectively, are also in condition for allowance.

Genty, Afek, Maeshima and Jorgensen

Applicant's dependent claims 12, 45 and 46 recite establishing a secure signaling channel between a source network device and a destination network device, sending via the secure signaling channel control packets between the source network device and the destination network device to monitor the performance of the first and second packet tunnels, and selecting a new intermediate network device when the performance reaches a minimum threshold. Applicant's dependent claim 13 recites maintaining a set of possible intermediate network devices for a plurality of available intermediate network devices.

The Examiner acknowledged that Genty, Afek and Maeshima do not disclose sending messages to monitor performance and making changes based on performance. However, the Examiner asserted that Jorgensen teaches monitoring, control, service, modify and repair a

system by sending messages monitoring the performance and making changes based on performance. The Examiner stated that it would have been obvious to one of ordinary skill in the art to use the monitoring described in Jorgensen with the system of Genty, Afek and Maeshima because protective provisioning of additional resources can occur.

As described above, Genty, Afek and Maeshima fail to disclose an intermediate network device that has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. Genty, Afek and Maeshima also fail to teach the remaining features of Applicant's independent claims 1 and 35. Jorgensen provides no teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima. Neither Genty, Afek, Maeshima nor Jorgensen disclose the features of Applicant's independent claims 1 and 35, which are in condition for allowance. For at least these reasons, Applicant's claims 12 and 13 which depend from claim 1, and claims 45 and 46 which depend from claim 35 are also in condition for allowance.

Genty, Afek, Maeshima and Shawcross

Applicant's dependent claims 16 and 29 recite establishing a packet tunnel by maintaining a set of available multicast network addresses, selecting one of the multicast network addresses for the packet tunnel, and subscribing to a multicast channel for the selected multicast network address. Applicant's dependent claim 17 recites establishing a second packet tunnel by unsubscribing to the multicast channel, selecting one of the multicast network addresses for the destination network address, establishing the second packet tunnel using the new destination address, and subscribing to a multicast channel for the selected multicast network address.

The Examiner acknowledged that Genty, Afek and Maeshima do not disclose the use of multicast addresses. However, the Examiner asserted that Shawcross teaches maintaining a set of multicast addresses, selecting a multicast address and subscribing to the multicast addresses. The Examiner stated that it would have been obvious to one of ordinary skill in the art to use the multicast addressing described in Shawcross with the system of Genty, Afek and Maeshima because the technique prevents unauthorized personnel from knowing which address to disrupt.

As described above, Genty, Afek and Maeshima fail to disclose an intermediate network device that has a network address from a network address space other than the address space of

the first local area network and the address space of the second local area network. Genty, Afek and Maeshima also fail to teach the remaining features of Applicant's independent claims 1 and 27. Shawcross provides no teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima. Neither Genty, Afek, Maeshima nor Shawcross disclose the features of Applicant's independent claims 1 and 27, which are in condition for allowance. For at least these reasons, Applicant's claims 16 and 17 which depend from claim 1, and claims 29 which depend from claim 27 are also in condition for allowance.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 1-4, 6, 7, 9-17, 27, 29, 30, 35-39, 41, 42, 44-46, 53 and 55 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

New Claims:

Applicant has added claims 57-60 to the pending application. The applied reference fails to disclose or suggest the inventions defined by Applicant's new claims, and provides no teaching that would have suggested the desirability of modification to arrive at the claimed inventions. For example, the reference fails to disclose or suggest *that the first local area network and the second local area network are separated by a public network, and the intermediate network device has a network address from a network address space of the public network*, as recited by Applicant's claims 57-60.

Support for new claims 57-60 is provided within Applicant's specification. For example, FIG. 3 illustrates public network 6 positioned between first local area network 14A and second local area network 14B. FIG. 3 also illustrates a tunnel concatenation device (TCD 42), i.e., an intermediate node, connected to public network 6. In addition, Applicant's specification recites that tunnel splitting increases the size of the unicast address space of the source to that of the unicast address space of the Internet (i.e., approximately 3.8 billion addresses).[4]

[4] Applicant's specification, page 13, lines 20-22.

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

September

By:

SHUMAKER & SIEFFERT, P.A.
1625 Radio Drive, Suite 300
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312